PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: WO 97/26732

(43) International Publication Date: 24 July 1997 (24.07.97)

(21) International Application Number: PCT/US97/00651

(22) International Filing Date: 16 January 1997 (16.01.97)

(30) Priority Data:
08/587,943 17 January 1996 (17.01.96) US

(71) Applicant: THE DICE COMPANY [US/US]; 20191 E. Country Club Drive, Townhouse 4, Aventura, FL 33180 (US).

(72) Inventors: MOSKOWITZ, Scott, A.; 20191 E. Country Club Drive, Townhouse 4, Aventura, FL 33180 (US). COOPERMAN, Marc; 2929 Ramona, Palo Alto, CA 94306 (US).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HU, IL, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR STEGA-CIPHER PROTECTION OF COMPUTER CODE

(57) Abstract

A method for protecting computer code copyrights by encoding the code into a data resource with a digital watermark. The digital watermark contains licensing information interwoven with essential code resources encoded into data resources. The result is that while an application program can be copied in an uninhibited manner, only the licensed user having the license code can access essential code resources to operate the program and any descendant copies bear the required license code.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

METHOD FOR STEGA-CIPHER PROTECTION OF COMPUTER CODE

FIELD OF INVENTION

With the advent of computer networks and digital multimedia, protection of intellectual property has become a prime concern for creators and publishers of digitized copies of copyrightable works, such as musical recordings, movies, video games, and computer software. One method of protecting copyrights in the digital domain is to use "digital watermarks."

The prior art includes copy protection systems attempted at many stages in the development of the software industry. These may be various methods by which a software engineer can write the software in a clever manner to determine if it has been copied, and if so to deactivate itself. Also included are undocumented changes to the storage format of the content. Copy protection was generally abandoned by the software industry, since pirates were generally just as clever as the software engineers and figured out ways to modify the software and deactivate the protection. The cost of developing such protection was not justified considering the level of piracy which occurred despite the copy protection.

Other methods for protection of computer software include the requirement of entering certain numbers or facts that may be included in a packaged software's manual, when prompted at start-up. These may be

overcome if copies of the manual are distributed to unintended users, or by patching the code to bypass these measures. Other methods include requiring a user to contact the software vendor and to receive "keys" for unlocking software after registration attached to some payment scheme, such as credit card authorization. Further methods include network-based searches of a user's hard drive and comparisons between what is registered to that user and what is actually installed on the user's general computing device. Other proposals, by such parties as AT&T's Bell Laboratories, use "kerning" or actual distance in pixels, in the rendering of text documents, rather than a varied number of ASCII characters. However, this approach can often be defeated by graphics processing analogous to sound processing, which randomizes that information. All of these methods require outside determination and verification of the validity of the software license.

Digital watermarks can be used to mark each individual copy of a digitized work with information identifying the title, copyright holder, and even the licensed owner of a particular copy. When marked with licensing and ownership information, responsibility is created for individual copies where before there was none. Computer application programs can be watermarked by watermarking digital content resources used in conjunction with images or audio data. Digital watermarks can be encoded with random or pseudo random keys, which act as secret maps for locating the watermarks. These keys make it impossible for a party to find the watermark without having the key. In addition, the encoding method can be enhanced to force a party to cause damage to a watermarked data stream when trying to erase a random-key watermark. Digital watermarks are described in "Steganographic Method and Device" - The DICE Company, Serial No. 08/489,172, the disclosure of which is hereby incorporated by reference.

Other information is disclosed in "Technology: Digital Commerce", Denise Caruso, New York Times, August 7, 1995; and "Copyrighting in the Information Age", Harley Ungar, ONLINE MARKETPLACE, September 1995, Jupiter Communications.

Additionally, other methods for hiding information signals in content signals, are disclosed in U.S. Patent No. 5,319,735 - Preuss et al. and U.S. Patent No. 5,379,345 - Greenberg.

It is desirable to use a "stega-cipher" or watermarking process to hide the necessary parts or resources of the executable object code in the digitized sample resources. It is also desirable to further modify the underlying structure of an executable computer application such that it is more resistant to attempts at patching and analysis by memory capture. A computer application seeks to provide a user with certain utilities or tools, that is, users interact with a computer or similar device to accomplish various tasks and applications provide the relevant interface. Thus, a level of authentication can also be introduced into software, or "digital products," that include digital content, such as audio, video, pictures or multimedia, with digital watermarks. Security is maximized because erasing this code watermark without a key results in the destruction of one or more essential parts of the underlying application, rendering the "program" useless to the unintended user who lacks the appropriate key. Further, if the key is linked to a license code by means of a mathematical function, a mechanism for identifying the licensed owner of an application is created.

It is also desirable to randomly reorganize program memory structure intermittently during program run time, to prevent attempts at memory capture or object code analysis aimed at eliminating licensing or ownership information, or otherwise modifying, in an unintended manner, the functioning of the application.

In this way, attempts to capture memory to determine underlying functionality or provide a "patch" to facilitate unauthorized use of the "application," or computer program, without destroying the functionality and thus usefulness of a copyrightable computer program can be made difficult or impossible.

It is thus the goal of the present invention to provide a higher level of copyright security to object code on par with methods described in digital watermarking systems for digitized media content such as pictures, audio, video and multimedia content in its multifarious forms, as described in previous disclosures, "Steganographic Method and Device" and "Human Assisted Random Key Generation and Application for Digital Watermark System", filed on even date herewith, the disclosure of which is hereby incorporated by reference.

It is a further goal of the present invention to establish methods of copyright protection that can be combined with such schemes as software metering, network distribution of code and specialized protection of software that is designed to work over a network, such as that proposed by Sun Microsystems in their HotJava browser and Java programming language, and manipulation of application code in proposed distribution of documents that can be exchanged with resources or the look and feel of the document being preserved over a network. Such systems are currently being offered by companies including Adobe, with their Acrobat software. This latter goal is accomplished primarily by means of the watermarking of font, or typeface, resources included in applications or documents, which determine how a bitmap representation of the document is ultimately drawn on a presentation device.

The present invention includes an application of the technology of "digital watermarks." As described in previous disclosures, "Steganographic Method and

Device" and "Human Assisted Random Key Generation and Application for Digital Watermark System," watermarks are particularly suitable to the identification, metering, distributing and authenticating digitized content such as pictures, audio, video and derivatives thereof under the description of "multimedia content." Methods have been described for combining both cryptographic methods, and steganography, or hiding something in plain view. Discussions of these technologies can be found in Applied Cryptography by Bruce Schneier and The Code Breakers by David Kahn. For more information on prior art public-key cryptosystems see US Pat No 4,200,770 Diffie-Hellman, 4,218,582 Hellman, 4,405,829 RSA, 4,424,414 Hellman Pohlig. Computer code, or machine language instructions, which are not digitized and have zero tolerance for error, must be protected by derivative or alternative methods, such as those disclosed in this invention, which focuses on watermarking with "keys" derived from license codes or other ownership identification information, and using the watermarks encoded with such keys to hide an essential subset of the application code resources.

SUMMARY OF THE INVENTION

It is thus a goal of the present invention, to provide a level of security for executable code on similar grounds as that which can be provided for digitized samples. Furthermore, the present invention differs from the prior art in that it does not attempt to stop copying, but rather, determines responsibility for a copy by ensuring that licensing information must be preserved in descendant copies from an original. Without the correct license information, the copy cannot function.

An improvement over the art is disclosed in the present invention, in that the software itself is a set of commands, compiled by software engineer, which can be

configured in such a manner as to tie underlying functionality to the license or authorization of the copy in possession by the user. Without such verification, the functions sought out by the user in the form of software cease to properly work. Attempts to tamper or "patch" substitute code resources can be made highly difficult by randomizing the location of said resources in memory on an intermittent basis to resist most attacks at disabling the system.

DETAILED DESCRIPTION

An executable computer program is variously referred to as an application, from the point of view of a user, or executable object code from the point of view of the engineer. A collection of smaller, atomic (or indivisible) chunks of object code typically comprise the complete executable object code or application which may also require the presence of certain data resources. These indivisible portions of object code correspond with the programmers' function or procedure implementations in higher level languages, such as C or Pascal. In creating an application, a programmer writes "code" in a higher level language, which is then compiled down into "machine language," or, the executable object code, which can actually be run by a computer, general purpose or otherwise. Each function, or procedure, written in the programming language, represents a self-contained portion of the larger program, and implements, typically, a very small piece of its functionality. The order in which the programmer types the code for the various functions or procedures, and the distribution of and arrangement of these implementations in various files which hold them is unimportant. Within a function or procedure, however, the order of individual language constructs, which correspond to particular machine instructions is important, and so functions or procedures are considered

indivisible for purposes of this discussion. That is, once a function or procedure is compiled, the order of the machine instructions which comprise the executable object code of the function is important and their order in the computer memory is of vital importance. Note that many "compilers" perform "optimizations" within functions or procedures, which determine, on a limited scale, if there is a better arrangement for executable instructions which is more efficient than that constructed by the programmer, but does not change the result of the function or procedure. Once these optimizations are performed, however, making random changes to the order of instructions is very likely to "break" the function. When a program is compiled, then, it consists of a collection of these sub-objects, whose exact order or arrangement in memory is not important, so long as any sub-object which uses another sub-object knows where in memory it can be found.

The memory address of the first instruction in one of these sub-objects is called the "entry point" of the function or procedure. The rest of the instructions comprising that sub-object immediately follow from the entry point. Some systems may prefix information to the entry point which describes calling and return conventions for the code which follows, an example is the Apple Macintosh Operating System (MacOS). These sub-objects can be packaged into what are referred to in certain systems as "code resources," which may be stored separately from the application, or shared with other applications, although not necessarily. Within an application there are also data objects, which consist of some data to be operated on by the executable code. These data objects are not executable. That is, they do not consist of executable instructions. The data objects can be referred to in certain systems as "resources."

When a user purchases or acquires a computer program, she seeks a computer program that "functions" in a desired manner. Simply, computer software is overwhelmingly purchased for its underlying functionality. In contrast, persons who copy multimedia content, such as pictures, audio and video, do so for the entertainment or commercial value of the content. The difference between the two types of products is that multimedia content is not generally interactive, but is instead passive, and its commercial value relates more on passive not interactive or utility features, such as those required in packaged software, set-top boxes, cellular phones, VCRs, PDAs, and the like. Interactive digital products which include computer code may be mostly interactive but can also contain content to add to the interactive experience of the user or make the underlying utility of the software more aesthetically pleasing. It is a common concern of both of these creators, both of interactive and passive multimedia products, that "digital products" can be easily and perfectly copied and made into unpaid or unauthorized copies. This concern is especially heightened when the underlying product is copyright protected and intended for commercial use.

The first method of the present invention described involves hiding necessary "parts" or code "resources" in digitized sample resources using a "digital watermarking" process, such as that described in the "Steganographic Method and Device" patent application. The basic premise for this scheme is that there are a certain sub-set of executable code resources, that comprise an application and that are "essential" to the proper function of the application. In general, any code resource can be considered "essential" in that if the program proceeds to a point where it must "call" the code resource and the code resource is not present in memory, or cannot be loaded, then the program fails.

However, the present invention uses a definition of "essential" which is more narrow. This is because, those skilled in the art or those with programming experience, may create a derivative program, not unlike the utility provided by the original program, by writing additional or substituted code to work around unavailable resources. This is particularly true with programs that incorporate an optional "plug-in architecture," where several code resources may be made optionally available at run-time. The present invention is also concerned with concentrated efforts by technically skilled people who can analyze executable object code and "patch" it to ignore or bypass certain code resources. Thus, for the present embodiment's purposes, "essential" means that the function which distinguishes this application from any other application depends upon the presence and use of the code resource in question. The best candidates for this type of code resources are NOT optional, or plug-in types, unless special care is taken to prevent work-a-rounds.

Given that there are one or more of these essential resources, what is needed to realize the present invention is the presence of certain data resources of a type which are amenable to the "stega-cipher" process described in the "Steganographic Method and Device" patent application. Data which consists of image or audio samples is particularly useful. Because this data consists of digital samples, digital watermarks can be introduced into the samples. What is further meant is that certain applications include image and audio samples which are important to the look and feel of the program or are essential to the processing of the application's functionality when used by the user. These computer programs are familiar to users of computers but also less obvious to users of other devices that run applications that are equivalent in

some measure of functionality to general purpose computers including, but not limited to, set-top boxes, cellular phones, "smart televisions," PDAs and the like. However, programs still comprise the underlying "operating systems" of these devices and are becoming more complex with increases in functionality.

One method of the present invention is now discussed. When code and data resources are compiled and assembled into a precursor of an executable program the next step is to use a utility application for final assembly of the executable application. The programmer marks several essential code resources in a list displayed by the utility. The utility will choose one or several essential code resources, and encode them into one or several data resources using the stega-cipher process. The end result will be that these essential code resources are not stored in their own partition, but rather stored as encoded information in data resources. They are not accessible at run-time without the key. Basically, the essential code resources that provide functionality in the final end-product, an executable application or computer program, are no longer easily and recognizably available for manipulation by those seeking to remove the underlying copyright or license, or its equivalent information, or those with skill to substitute alternative code resources to "force" the application program to run as an unauthorized copy. For the encoding of the essential code resources, a "key" is needed. Such a key is similar to those described in the "Steganographic Method and Device." The purpose of this scheme is to make a particular licensed copy of an application distinguishable from any other. It is not necessary to distinguish every instance of an application, merely every instance of a license. A licensed user may then wish to install multiple copies of an application, legally or with authorization. This method, then, is to

choose the key so that it corresponds, is equal to, or is a function of, a license code or license descriptive information, not just a text file, audio clip or identifying piece of information as desired in digital watermarking schemes extant and typically useful to stand-alone, digitally sampled content. The key is necessary to access the underlying code, i.e., what the user understands to be the application program.

The assembly utility can be supplied with a key generated from a license code generated for the license in question. Alternatively, the key, possibly random, can be stored as a data resource and encrypted with a derivative of the license code. Given the key, it encodes one or several essential resources into one or several data resources. Exactly which code resources are encoded into which data resources may be determined in a random or pseudo random manner. Note further that the application contains a code resource which performs the function of decoding an encoded code resource from a data resource. The application must also contain a data resource which specifies in which data resource a particular code resource is encoded. This data resource is created and added at assembly time by the assembly utility. The application can then operate as follows:

1) when it is run for the first time, after installation, it asks the user for personalization information, which includes the license code. This can include a particular computer configuration;

2) it stores this information in a personalization data resource;

3) Once it has the license code, it can then generate the proper decoding key to access the essential code resources.

Note that the application can be copied in an uninhibited manner, but must contain the license code issued to the licensed owner, to access its essential code resources. The goal of the invention, copyright

protection of computer code and establishment of responsibility for copies, is thus accomplished.

This invention represents a significant improvement over prior art because of the inherent difference in use of purely informational watermarks versus watermarks which contain executable object code. If the executable object code in a watermark is essential to an application which accesses the data which contains the watermark, this creates an all-or-none situation. Either the user must have the extracted watermark, or the application cannot be used, and hence the user cannot gain full access to the presentation of the information in the watermark bearing data. In order to extract a digital watermark, the user must have a key. The key, in turn, is a function of the license information for the copy of the software in question. The key is fixed prior to final assembly of the application files, and so cannot be changed at the option of the user. That, in turn, means the license information in the software copy must remain fixed, so that the correct key is available to the software. The key and the license information are, in fact, interchangeable. One is merely more readable than the other. In the earlier developed "Steganographic Method and Device," the possibility of randomization erasure attacks on digital watermarks was discussed. Simply, it is always possible to erase a digital watermark, depending on how much damage you are willing to do to the watermark-bearing content stream. The present invention has the significant advantage that you must have the watermark to be able to use the code it contains. If you erase the watermark you have lost a key piece of the functionality of the application, or even the means to access the data which bear the watermark.

A preferred embodiment would be implemented in an embedded system, with a minimal operating system and

memory. No media playing "applets," or smaller sized applications as proposed in new operating environments envisioned by Sun Microsystems and the advent of Sun's Java operating system, would be permanently stored in the system, only the bare necessities to operate the device, download information, decode watermarks and execute the applets contained in them. When an applet is finished executing, it is erased from memory. Such a system would guarantee that content which did not contain readable watermarks could not be used. This is a powerful control mechanism for ensuring that content to be distributed through such a system contains valid watermarks. Thus, in such networks as the Internet or set-top box controlled cable systems, distribution and exchange of content would be made more secure from unauthorized copying to the benefit of copyright holders and other related parties. The system would be enabled to invalidate, by default, any content which has had its watermark(s) erased, since the watermark conveys, in addition to copyright information, the means to fully access, play, record or otherwise manipulate, the content.

A second method according to the present invention is to randomly re-organize program memory structure to prevent attempts at memory capture or object code analysis. The object of this method is to make it extremely difficult to perform memory capture-based analysis of an executable computer program. This analysis is the basis for a method of attack to defeat the system envisioned by the present invention.

Once the code resources of a program are loaded into memory, they typically remain in a fixed position, unless the computer operating system finds it necessary to rearrange certain portions of memory during "system time," when the operating system code, not application code, is running. Typically, this is done in low memory systems, to maintain optimal memory utilization. The

MacOS for example, uses Handles, which are double-indirect pointers to memory locations, in order to allow the operating system to rearrange memory transparently, underneath a running program. If a computer program contains countermeasures against unlicensed copying, a skilled technician can often take a snapshot of the code in memory, analyze it, determine which instructions comprise the countermeasures, and disable them in the stored application file, by means of a "patch." Other applications for designing code that moves to prevent scanning-tunnelling microscopes, and similar high sensitive hardware for analysis of electronic structure of microchips running code, have been proposed by such parties as Wave Systems. Designs of Wave Systems' microchip are intended for preventing attempts by hackers to "photograph" or otherwise determine "burn in" to microchips for attempts at reverse engineering. The present invention seeks to prevent attempts at understanding the code and its organization for the purpose of patching it. Unlike systems such as Wave Systems', the present invention seeks to move code around in such a manner as to complicate attempts by software engineers to reengineer a means to disable the methods for creating licensed copies on any device that lacks "trusted hardware." Moreover, the present invention concerns itself with any application software that may be used in general computing devices, not chipsets that are used in addition to an underlying computer to perform encryption. Wave Systems' approach to security of software, if interpreted similarly to the present invention, would dictate separate microchip sets for each piece of application software that would be tamperproof. This is not consistent with the economics of software and its distribution.

Under the present invention, the application contains a special code resource which knows about all the other code resources in memory. During execution

time, this special code resource, called a "memory scheduler," can be called periodically, or at random or pseudo random intervals, at which time it intentionally shuffles the other code resources randomly in memory, so that someone trying to analyze snapshots of memory at various intervals cannot be sure if they are looking at the same code or organization from one "break" to the next. This adds significant complexity to their job. The scheduler also randomly relocates itself when it is finished. In order to do this, the scheduler would have to first copy itself to a new location, and then specifically modify the program counter and stack frame, so that it could then jump into the new copy of the scheduler, but return to the correct calling frame. Finally, the scheduler would need to maintain a list of all memory addresses which contain the address of the scheduler, and change them to reflect its new location.

The methods described above accomplish the purposes of the invention - to make it hard to analyze captured memory containing application executable code in order to create an identifiable computer program or application that is different from other copies and is less susceptible to unauthorized use by those attempting to disable the underlying copyright protection system. Simply, each copy has particular identifying information making that copy different from all other copies.

What is Claimed Is:

1. A method of associating executable object code with a digital sample stream by means of a digital watermark wherein the digital watermark contains executable object code and is encoded into the digital sample stream.

2. The method of claim 1 wherein a key to access the digital watermark is a function of a collection of license information pertaining to the software which is accessing the watermark

where license information consists of one or more of the following items:

Owning Organization name;
Personal Owner name;
Owner Address;
License code;
Software serialization number;
Distribution parameters;
Appropriate executable general computing device architecture;
Pricing; and
Software Metering details.

3. The method of claim 1 further comprising the step of transmitting the digital sample stream, via a transmission means, from a publisher to a subscriber

wherein transmission means can selected from the group of

soft sector magnetic disk media;
hard sector magnetic disk media;
magnetic tape media;
optical disc media;
Digital Video Disk media;
magneto-optical disk media;
memory cartridge;
telephone lines;

SCSI;
Ethernet or Token Ring Network;
ISDN;
ATM network;
TCP/IP network;
analog cellular network;
digital cellular network;
wireless network;
digital satellite;
cable network;
fiber optic network; and
electric powerline network.

4. The method of claim 1 where the object code to be encoded is comprised of series of executable machine instructions which perform the function of processing a digital sample stream for the purpose of modifying it or playing the digital sample stream.

5. The method of claim 3 further comprising the steps of:
decoding said digital watermark and extracting object code;
loading object code into computer memory for the purpose of execution;
executing said object code in order to process said digital sample stream for the purpose of playback.

6. A method of assembling an application to be protected by watermark encoding of essential resources comprising the steps of:
assembling a list of identifiers of essential code resources of an application where identifiers allow the code resource to be accessed and loaded into memory;
providing license information on the licensee who is to receive an individualized copy of the application;

storing license information in a personalization resource which is added to the list of application data resources;

generating a digital watermark key from the license information; using the key as a pseudo-random number string to select a list of suitable digital sample data resources, the list of essential code resources, and a mapping of which essential code resources are to be watermarked into which data resources;

storing the map, which is a list of paired code and data resource identifiers, as a data resource, which is added to the application;

adding a digital watermark decoder code resource to the application, to provide a means for extracting essential code resource from data resources, according to the map;

processing the map list and encoding essential code resources into digital sample data resources with a digital watermark encoder;

removing self-contained copies of the essential code resources which have been watermarked into data resources; and

combining all remaining code and data resources into a single application or installer.

7. A method of intermittently relocating application code resources in computer memory, in order to prevent, discourage, or complicate attempts at memory capture based code analysis.

8. The method of claim 7 additionally comprising the step of

assembling a list of identifiers of code resources of an application where identifiers allow the code resource to be accessed and loaded into memory.

9. The method of claim 8 additionally comprising the step of modifying application program structure to make all code resource calls indirectly, through the memory scheduler, which looks up code resources in its list and dispatches calls.

10. The method of claim 9 additionally comprising the step of intermittently rescheduling or shuffling all code resources prior to or following the dispatch of a code resource call through the memory scheduler.

11. The method of claim 10 additionally comprised of the step of the memory scheduler copying itself to a new location in memory.

12. The method of claim 11 additionally comprising the step of modifying the stack frame, program counter, and memory registers of the CPU to cause the scheduler to jump to the next instruction comprising the scheduler, in the copy, to erase the previous memory instance of the scheduler, and changing all memory references to the scheduler to reflect its new location, and to return from the copy of the scheduler to the frame which called the previous copy of the scheduler.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00651

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL : 380/54
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/54, 2, 4, 9, 21, 23, 25, 28, 49, 50, 59; 283/73, 113, 17

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,349,655 A (MANN) 20 September 1994, see Abstract.	1
X	US 4,262,329 A (BRIGHT et al) 14 April 1981, see Abstract.	7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 04 APRIL 1997	Date of mailing of the international search report 29 APR 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer for BERNARR EARL GREGORY Telephone No. (703) 306-4153

Form PCT/ISA/210 (second sheet)(July 1992)*